CLAIMS

Sub A1

1. A method of enabling a proxy to participate in a secure communication between a client and a server, comprising the step of:

establishing a first secure session between the client and the proxy;

upon verifying the first secure session, establishing a second secure session between the client and the proxy, the second secure session requesting the proxy to act as a conduit to the server;

having the client and the server negotiate a session master secret; and

delivering the session master secret to the proxy using the first secure session to enable the proxy to participate in the secure communication.

2. The method as described in **Claim 1** further including the step of having the proxy use the session master secret and a session identifier to generate given cryptographic information.

3. The method as described in **Claim 2** further including the step of having the proxy enter an active operating state following receipt of the session master secret and generation of the given cryptographic information.

4. The method as described in **Claim 3** wherein the proxy performs a given service on behalf of the client in the active operating state.

5. The method as described in **Claim 4** wherein the given service is selected from a set of services including transcoding, caching, encryption, decryption, monitoring, filtering and pre-fetching.

6. The method as described in **Claim 1** wherein the first and second secure sessions confirm to a network security protocol.

7. The method as described in **Claim 6** wherein the network security protocol is SSL.

8. The method as described in **Claim 6** wherein the network security protocol is TLS.

9. The method as described in **Claim 1** wherein the server is a Web server and the client is a pervasive computing client.

10. A method of enabling a proxy to participate in a secure communication between a client and a server, comprising the step of:

having the client request a first secure connection to the proxy;

upon authenticating validity of a certificate received from the proxy, having the client request a second secure connection to proxy, the second secure connection requesting the proxy to act as a conduit to the server;

having the proxy generate a session identifier;

having the client and the server negotiate a session master secret through the conduit;

upon completion of the negotiation, having the client deliver the session master secret to the proxy using the first secure connection;

having the proxy use the session master secret and the session identifier to generate given cryptographic information that is useful for participating in the secure communication.

11. The method as described in **Claim 10** further including the step of having the proxy enter an active operating state following receipt of the session master secret and generation of the given cryptographic information.

12. The method as described in **Claim 11** wherein the proxy performs a given service on behalf of the client in the active operating state.

13. The method as described in **Claim 12** wherein the given service is selected from a set of services including transcoding, caching, encryption, decryption, monitoring, filtering and pre-fetching.

14. The method as described in **Claim 10** wherein the first and second secure sessions confirm to a network security protocol.

15. The method as described in **Claim 14** wherein the network security protocol is SSL.

16. The method as described in **Claim 14** wherein the network security protocol is TLS.

17. A method for establishing the security of a session between a client and a server, comprising the steps of:

through a proxy, conducting a security handshake procedure between the client and the server to produce a session key; and

transmitting the session key to the proxy so that the proxy can participate in communications between the client and the server during the session.

18. The method as described in **Claim 17** wherein the session key is transmitted from the client to the proxy over a secure connection.

19. The method as described in **Claim 18** wherein the secure connection between the client and the proxy is created before the security handshake procedure and is maintained throughout the session.

20. A cryptographic system, comprising:

a client;

a server;

a proxy;

a network protocol service for enabling the client and server to communicate over a secure connection;

a computer program (i) for controlling the client to request a first secure connection to the proxy, (ii) responsive to authenticating validity of a certificate from the proxy, for controlling the client to request a second secure connection to proxy, the second secure connection requesting the proxy to act as a conduit to the server, (iii) for controlling the client to negotiate with the server through the conduit to obtain a session master; and (iv) upon successful completion of the negotiation, for controlling the client to deliver the session master secret to the proxy using the first secure connection; and

a computer program (i) for controlling the proxy to use the session master secret and a session identifier to generate given cryptographic information, and (ii) for switching the proxy into an active operating state during which it can participate in communications between the client and the server.

Rule 126

21 22. The cryptographic system as described in **Claim 21** wherein the proxy includes means for providing transcoding services on behalf of the client.

22 23. The cryptographic system as described in **Claim 21** wherein the proxy includes means for providing encryption/decryption services on behalf of the client.

23 24. The cryptographic system as described in **Claim 21** wherein the proxy includes means for providing caching services on behalf of the client.

24 25. The cryptographic system as described in **Claim 21** wherein the proxy includes means for providing monitoring services on behalf of the client.

25 26. A computer program product in a computer readable medium for use in a cryptographic system including a client, a server, and a proxy, comprising:

a first routine (i) for controlling the client to request a first secure connection to the proxy, (ii) responsive to authenticating validity of a certificate from the proxy, for controlling the client to request a second secure connection to proxy, the second secure connection requesting the proxy to act as a conduit to the server, (iii) for controlling the client to negotiate with the server through the conduit to obtain a session master; and (iv) upon successful completion of the negotiation, for controlling the client to deliver the session master secret to the proxy using the first secure connection; and

a second routine (i) for controlling the proxy to use the session master secret and a session identifier to generate given cryptographic information, and (ii) for switching the proxy into an active operating state during which it can participate in communications between the client and the server.